대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0029144
Application Number

출 원 년 월 일 : 2003년 05월 07일
Date of Application MAY 07, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 03 월 02 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0006
【제출일자】	2003.05.07
【발명의 명칭】	컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법
【발명의 영문명칭】	A METHOD FOR VERIFICATING THE INTEGRITY OF CODED CONTENTS AND AUTHENTICATING THE CONTENTS PROVIDER
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【발명자】	
【성명의 국문표기】	장경아
【성명의 영문표기】	CHANG,Kyung Ah
【주민등록번호】	740818-2023611
【우편번호】	136-041
【주소】	서울특별시 성북구 삼선동1가 188번지 9통 6반 4층
【국적】	KR
【발명자】	
【성명의 국문표기】	이병래
【성명의 영문표기】	LEE,Byung Rae
【주민등록번호】	750519-1069422
【우편번호】	449-843
【주소】	경기도 용인시 수지읍 상현리 만현마을 성원상떼빌 306동 104호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 김동진 (인)

【수수료】

【기본출원료】	16	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	8	항	365,000 원
【합계】	394,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 유무선 통신망을 통해 다양한 멀티미디어 컨텐츠를 다운로드 받거나 교환 및 전달 시 컨텐츠 제공자를 인증하고 컨텐츠의 무결성을 보장하기 위한 방법에 관한 것이다. 상기 컨텐츠 제공자 인증과 컨텐츠 무결성을 보장하기 위해서, 본 발명의 패키지화 된 컨텐츠는 암호화 된 컨텐츠부와 컨텐츠 제공자의 인증서를 얻을 수 있는 주소가 포함된 헤더부로 이루어지며, 컨텐츠의 무결성을 보장하기 위해서 상기 헤더부와 컨텐츠부가 해쉬 부호화되어 전자서명이 이루어져 있다.

상기 컨텐츠를 이용하여, 본 발명의 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법은 전자서명이 이루어진 패키지화 된 컨텐츠를 유무선 통신망을 통해 사용자의 디바이스에 다운로드 받는 단계와, 상기 컨텐츠의 헤더부에서 컨테츠 제공자의 서명 검증을 위해 인증서가 제공되는 URL 주소를 파악하는 단계와, 상기 URL 주소로 이동하여 상기 컨텐츠 제공자의 인증서를 획득하는 단계와, 상기 획득한 인증서로부터 상기 전자서명을 검증하는데 필요한 공개키를 추출하는 단계, 및 상기 추출된 공개키를 이용하여 상기 전자서명을 검증하는 단계로 이루어진다.

그 결과, 본 발명은 컨텐츠 수신자는 전자서명의 검증을 통해 컨텐츠 제공자를 인증하고, 해당 컨텐츠에 대한 무결성을 검증할 수 있는 효과를 기대할 수 있다.

【대표도】

도 4

【색인어】

컨텐츠, 전자서명, 헤더, 인증, 검증, 해쉬 함수, DRM, 공개키

【명세서】

【발명의 명칭】

컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법{A METHOD FOR VERIFICATING THE INTEGRITY OF CODED CONTENTS AND AUTHENTICATING THE CONTENTS PROVIDER}

【도면의 간단한 설명】

도 1은 종래의 패키지화 된 컨텐츠의 구성도.

도 2는 본 발명에 따른 패키지화 된 컨텐츠의 구성도.

도 3은 본 발명에 따른 컨테츠 제공자의 인증 과정을 나타낸 블록도.

도 4는 본 발명에 따른 컨텐츠 제공자를 인증하고 컨텐츠의 무결성을 보장하기 위한 방법을 나타낸 순서도.

< 도면의 주요부분에 대한 부호의 설명 >

1, 10: 패키지화 된 컨텐츠 2, 11: 컨텐츠부

3, 12: 헤더부 4, 13: 전자서명

20: 컨텐츠 제공자(CP) 30: 인증기관(CA)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법에 관한 것으로, 보다 상세하게는, 유무선 통신망을 통해 다양한 멀티미디어 컨텐츠를 다운로드 받거나 교환 및 전달 시 컨텐츠 제공자를 인증하고 컨텐츠의 무결성을 보장하기 위한 방법에 관한 것이다.

<10> 현재, 유무선 통신망을 이용하여 다양한 컨텐츠의 유통이 이루어지는데, 디지털 컨텐츠의 저작권을 보호하기 위해 다양한 기술 개발이 활발히 진행되고 있다. 이와 관련한 대표적인 기술로 DRM(Digital Rights Management: 디지털 저작권 관리)이 있는데, 예를 들어 마이크로소프트의 DRM(Digital Rights Management)와 OMA(Open Mobile Alliance) DRM v1.0 등이 있다.

<11> 이와 관련하여, 종래에는, DRM 기능이 있는 디바이스를 이용하는 사용자가 유무선 통신망을 이용하여 패키지화 된 컨텐츠를 다운로드 받거나 다른 사용자의 디바이스로 파일전송, 게시판, 또는 이메일 등을 통하여 자유롭게 교환 및 전송하는 경우 해당 컨텐츠에 대한 무결성을 보장하기 위한 기술이 있다.

<12> 도 1은 종래의 패키지화 된 컨텐츠(1)의 구성도를 나타낸다. 상기 컨텐츠(1)는 암호화된 컨텐츠부(2), 해당 컨텐츠의 각종 정보를 포함한 헤더부(3), 및 컨텐츠(1)의 헤더부(3)에 대해 해쉬(hash) 부호화 된 전자서명(4)으로 이루어진다. 도 1에 도시된 바와 같이, 상기 컨텐츠부(2)는 암호화 되어 있으며, 상기 헤더부(3)에는 컨텐츠 제공자(Contents Provider: CP)의 이름, 컨텐츠의 아이디, 메타 정보, 및 라이센스 제공자 URL 등이 포함되어 있다. 여기서, 전자서명(4)에 있어서 일반적으로 해쉬 함수를 사용하고 있는데, 이는 '임의의 길이를 가진 이진 스트링들을 해쉬값이라 불리는 어떤 고정된 길이의 이진 스트링으로 사상하는 계산적으로 효과적인 함수'라고 설명될 수 있다. 이러한 해쉬 함수는 전자서명(4)에 사용되는 것 외에도 데이터 무결성을 위해 사용될 수 있다.

<13> 예를 들어, 상기 컨텐츠(1)의 헤더부(3)에 대해 미리 해쉬 함수로 부호화하여 전자서명(4)을 포함한 컨텐츠(1)를 다운로드 받게 되면, 이 컨텐츠(1)에 해쉬 함수를 적용한 후 상기 전자서명(4)과 상기 컨텐츠 제공자를 통해 제공된 공개키와 비교함으로써, 전자서명을 검증할 수 있다.

<14> 이와 같이, 유무선 통신망을 통해 사용자가 상기 패키지화 된 컨텐츠(1)를 상기 컨텐츠 제공자로부터 다운로드 받거나 다른 사용자로부터 전송 받을 경우, 헤더부(3)에 대해 미리 해쉬화 한 전자서명(4)이 되어 있는 상기 헤더부(3)와 함께 상기 컨텐츠부(2)가 전송되므로, 상기 패키지화 된 컨텐츠(1)에 대한 무결성이 보장된다.

<15> 하지만, 이와 같은 종래 기술 방식에서는 상기 헤더부(3)에 대해서만 해쉬 부호화 되어 전자서명(4)이 이루어진 것으로, 상기 컨텐츠부(2)와 헤더부(3)와의 상호 연결성에 대한 무결성은 보장할 수 없다는 문제점이 있다.

<16> 또한, 전달 받은 컨텐츠(1)가 정당한 컨텐츠 제공자가 만든 것인지 인증할 수 없으며, 패키지화 된 컨텐츠(1)의 무결성을 검증하기 위해 필요한 컨텐츠 제공자의 공개키 인증서를 획득할 방법이 없다는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<17> 본 발명은 상기한 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은 전자서명을 검증할 수 있게 헤더부에 컨텐츠 제공자의 인증서를 획득할 수 있는 URL(Uniform Resource Locator) 주소를 포함함으로써, 이를 통해 컨텐츠 제공자의 인증서를 획득하여 컨텐츠 제공자를 인증하고 컨텐츠의 무결성을 보장하기 위한 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<18> 상기 목적을 달성하기 위하여 안출된 것으로, 본 발명은, 암호화 된 컨텐츠부, 및 컨텐츠 제공자의 인증서를 얻을 수 있는 주소가 포함된 헤더부로 이루어진 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장을 위한 패키지화 된 컨텐츠 구조를 제공하고자 한다.

<19> 더 나아가, 본 발명은, 전자서명이 이루어진 패키지화 된 컨텐츠를 유무선 통신망을 통해 사용자의 디바이스에 다운로드 받는 단계; 상기 컨텐츠의 헤더부에서 컨테츠 제공자의 서명 검증을 위해 인증서가 제공되는 URL 주소를 파악하는 단계; 상기 URL 주소로 이동하여 상기 컨텐츠 제공자의 인증서를 획득하는 단계; 상기 획득한 인증서로부터 상기 전자서명을 검증하는데 필요한 공개키를 추출하는 단계; 및 상기 추출된 공개키를 이용하여 상기 전자서명을 검증하는 단계로 이루어진 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법을 제공하고자 한다.

<20> 이하, 첨부한 도면들을 참조로 본 고안의 바람직한 실시예를 목적 및 구성과 관련하여 상세히 설명한다.

<21> 도 2는 패키지화 된 컨텐츠(10)의 구성도를 나타낸다. 상기 컨텐츠(10)는, 도 2에 도시된 바와 같이, 암호화 된 컨텐츠부(11), 컨텐츠에 대한 각종 정보를 포함한 헤더부(12), 및 컨텐츠 제공자(20)의 인증서를 얻을 수 있는 주소와 무결성을 보장하기 위한 전자서명(13)으로 이루어진다.

<22> 상기 헤더부(12)에는 컨텐츠를 사용자에게 분배하는 컨텐츠 제공자(Contents Provider: CP)(20)의 이름, 컨텐츠 아이디, 라이센스 제공자 URL, 및 컨텐츠 제공자(20)의 인증서를 획득할 수 있는 URL 주소 등이 포함되어 있다. 여기서, 상기 컨텐츠 제공자(20)의 인증서를 제공하는 URL 주소가 포함되어 있는 것이 특징으로, 이를 통해 컨텐츠 제공자(20)의 인증서를 획득할 수 있어, 컨텐츠 제공자(20)가 해당 컨텐츠를 제공한 정확한 제공자인지의 여부를 검증할 수 있다.

<23> 상기 패키지화 된 컨텐츠(10)의 무결성 보장과 컨텐츠 제공자(20)의 인증을 위해서 컨텐츠 제공자(20)는 상기 헤더부(12)와 컨텐츠부(11)에 대해 해쉬(hash) 부호화한 전자서명(13)을

상기 패키지화 된 컨텐츠(10)에 삽입한다. 만약, 상기 컨텐츠부(11)의 크기가 커서 해쉬 부호화하여 전자서명(13)을 하기에 어려운 경우에는 상기 컨텐츠부(11)의 일부분만 해쉬 부호화하여 상기 헤더부(12)와 함께 전자 서명을 할 수 있다.

<24> 도 3은 상기 패키지화 된 컨텐츠(10)의 헤더부(12)의 정보를 이용하여 컨텐츠 제공자(20)의 인증서를 획득하는 과정을 나타낸 개략적인 블록도이다.

<25> 컨텐츠 제공자(20)는 상기 헤더부(12)와 암호화 된 컨텐츠부(11)에 대해 해쉬 부호화하여 전자서명(13)을 상기 패키지화 된 컨텐츠(10)에 삽입하고, 상기 전자서명(13)을 검증하는데 필요한 공개키를 해당 인증기관(Certification Authority: CA)(30)에 미리 받은 인증서에 제공한다. 그리고, 사용자(B)는 상기 컨텐츠 제공자(CP)(20) 또는 사용자(A)로부터 상기 컨텐츠(10)를 다운로드 받게 되면, 상기 컨텐츠 제공자(20)의 인증서가 제공되는 URL(Uniform Resource Locator: URL) 이용하여 컨텐츠 제공자(20)의 인증서를 획득하여 공개키를 추출한다. 이렇게 추출된 공개키의 값과 상기 컨텐츠(10)에 대해 해쉬 부호화한 해쉬값과 비교하여 전자서명(13)을 검증함으로써, 컨텐츠 제공자(20)에 대한 인증이 가능해지고 상기 컨텐츠(13)의 무결성이 보장될 수 있다.

<26> 도 4는 유무선 통신망을 통해 DRM 기능이 있는 디바이스에서의 컨텐츠 제공자(20)의 인증 및 컨텐츠의 무결성 보장 방법에 관한 순서도이다. 여기서, 기존의 통신망을 통해 다양한 멀티미디어 컨텐츠들을 교환 및 전달하기 위해 일반적으로 컨텐츠 제공자(20)들은 미리 인증기관(30)의 전자서명으로 인증을 받은 인증서를 소유하고 있으며, 상기 컨텐츠 제공자(20)들의 인증서를 검증할 수 있는 사용자의 공개키를 사전에 보유하고 있다. 이 경우, 사용자가 패키지화 된 컨텐츠(10)를 받아서 검증하는 방법에 대해 설명한다.

<27> 우선, 헤더부와 암호화된 컨텐츠부가 해쉬 부호화 되어 전자서명이 이루어진 패키지화 된 컨텐츠를 유무선 통신망을 통해 사용자의 디바이스에 다운로드 받는다(S10).

<28> 다음으로, 다운로드 받은 상기 컨텐츠(10)를 받아 상기 헤더부(12)에서 컨테츠 제공자(20)의 서명 검증을 위한 인증서가 제공되는 URL 주소를 파악한다(S20).

<29> 상기 URL 주소를 파악한 후, 상기 컨텐츠 제공자(20)의 인증서를 획득하기 위해 상기 URL 주소로 이동하여 상기 컨텐츠 제공자(20)의 인증서를 획득한다(S30).

<30> 그 다음으로, 획득된 상기 컨텐츠 제공자(20)의 인증서에서 상기 전자서명(13)을 검증하는데 필요한 공개키를 추출한다(S40).

<31> 그리고, 상기 추출된 공개키를 이용하여 상기 전자서명을 검증하게 된다(S50).

<32> 상기 검증 단계에서 검증이 성공되면, 상기 헤더부(12)와 컨텐츠부(11)의 상호 연결성을 보장하는 무결성이 보장되고 상기 컨텐츠 제공자(20)가 정당한 컨텐츠 제공자인지를 인증할 수 있게 된다.

<33> 상기 전자서명(13)을 검증하는 단계에서는 상기 패키지화 된 컨텐츠(10)에 해쉬 함수를 적용하여 상기 전자서명(13)과 비교하는 단계를 포함할 수 있다.

<34> 또한, 상기 전자서명(13)은 상기 헤더부(12)와 상기 암호화된 컨텐츠부(11)에 대해 해쉬 부호화하여 상기 컨텐츠(10)에 삽입되며, 이 경우 상기 컨텐츠부(11)는 전체 또는 일부분만을 해쉬 부호화할 수 있다.

<35> 상기 컨텐츠(10)에 해쉬 함수를 적용한 해쉬값과 상기 추출된 공개키의 값과 비교하여 전자서명을 검증한다.

<36> 상기 살펴 본 바와 같이, 패키지화 된 컨텐츠(10)의 헤더부(12)를 통하여 컨텐츠 제공자(20)의 인증서를 획득한 후, 이를 이용하여 전자서명(13)을 검증함으로써 컨텐츠(10)의 무결성을 검증하고 컨텐츠 제공자(20)를 인증할 수 있게 된다.

<37> 이상에서 본 발명에 대하여 상세히 기술하였지만, 본 발명이 속하는 기술 분야에 있어서 통상의 지식을 가진 사람이라면, 첨부된 청구범위에 정의된 본 발명의 정신 및 범위를 벗어나지 않으면서 본 발명을 여러 가지로 변형 또는 변경하여 실시할 수 있음은 자명하며, 따라서 본 발명의 실시예에 따른 단순한 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

【발명의 효과】

<38> 상기한 구성의 본 발명에 의하면, 컨텐츠 수신자는 헤더와 컨텐츠의 연관성을 보장하는 무결성을 확인함으로써 올바른 컨텐츠의 수신을 확인할 수 있으며, 패키지화 된 컨텐츠의 해쉬값에 대한 전자서명을 검증함으로써 정당한 컨텐츠 제공자가 제공한 것인지에 대한 확신과 컨텐츠의 무결성을 검증할 수 있는 효과를 기대할 수 있다.

【특허청구범위】

【청구항 1】

암호화 된 컨텐츠부, 및

컨텐츠 제공자의 인증서를 얻을 수 있는 주소가 포함된 헤더부로 이루어진 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장을 위한 패키지화 된 컨텐츠 구조.

【청구항 2】

제 1항에 있어서, 상기 패키지화 된 컨텐츠에 대한 무결성을 보장하기 위해 상기 헤더부와 컨텐츠부의 소정 부분을 해쉬(hash) 부호화하여 삽입된 전자서명을 더 포함하는 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장을 위한 패키지화 된 컨텐츠 구조.

【청구항 3】

제 2항에 있어서, 상기 전자서명은 상기 컨텐츠부의 일부분만 해쉬 부호화하여 전자서명에 포함하는 것을 특징으로 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장을 위한 패키지화 된 컨텐츠 구조.

【청구항 4】

제 1항에 있어서, 상기 헤더부는 컨텐츠 제공자 이름, 컨텐츠 아이디, 라이센스 제공자 URL, 및 메타 정보 등을 더 포함하는 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장을 위한 패키지화 된 컨텐츠 구조.

【청구항 5】

전자서명이 이루어진 패키지화 된 컨텐츠를 유무선 통신망을 통해 사용자의 디바이스에 다운로드 받는 단계;

상기 컨텐츠의 헤더부에서 컨텐츠 제공자의 서명 검증을 위해 인증서가 제공되는 URL 주소를 파악하는 단계;

상기 URL 주소로 이동하여 상기 컨텐츠 제공자의 인증서를 획득하는 단계;

상기 획득한 인증서로부터 상기 전자서명을 검증하는데 필요한 공개키를 추출하는 단계 ; 및

상기 추출된 공개키를 이용하여 상기 전자서명을 검증하는 단계로 이루어진 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법.

【청구항 6】

제 5항에 있어서, 상기 전자서명을 검증하는 단계는, 상기 패키지화 된 컨텐츠에 해쉬 함수를 적용하여 상기 전자서명과 비교하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법.

【청구항 7】

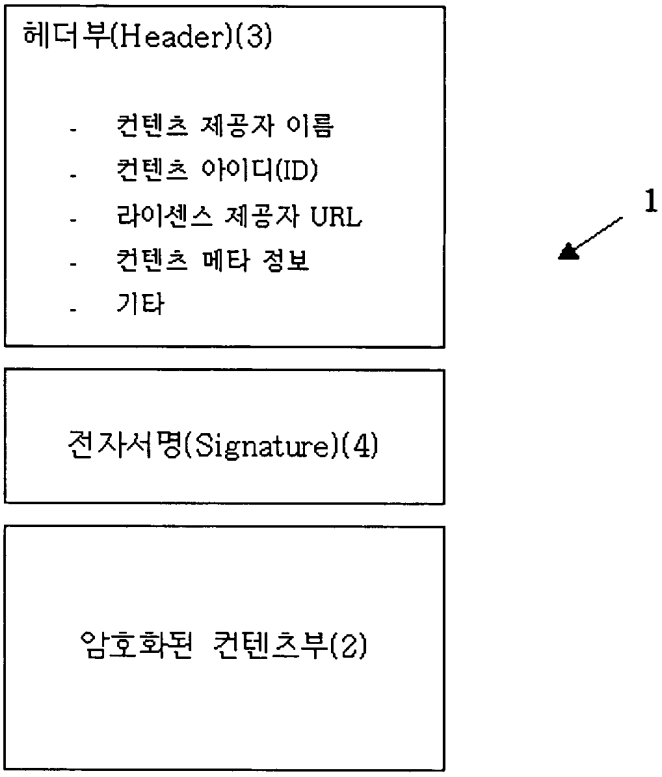
제 5항에 있어서, 상기 전자서명은 상기 헤더부와 암호화된 컨텐츠부에 대해 해쉬 부호화하여 상기 컨텐츠에 삽입되는 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장방법.

【청구항 8】

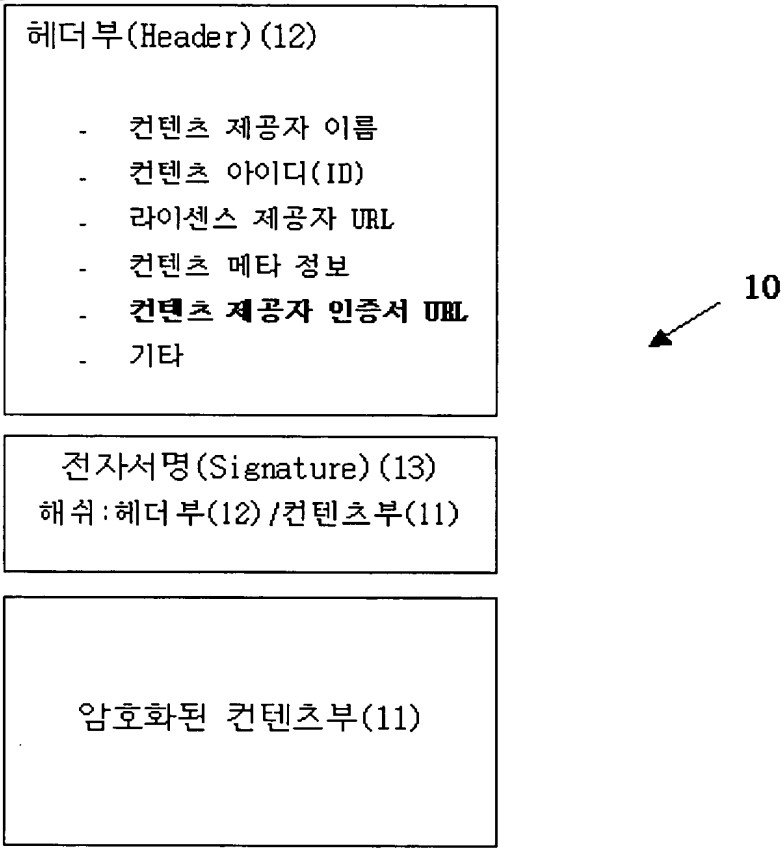
제 7항에 있어서, 상기 전자서명은 상기 컨텐츠부의 일부만 해쉬 부호화하여 상기 컨텐츠에 삽입되는 것을 특징으로 하는 컨텐츠 제공자 인증 및 컨텐츠 무결성 보장 방법.

【도면】

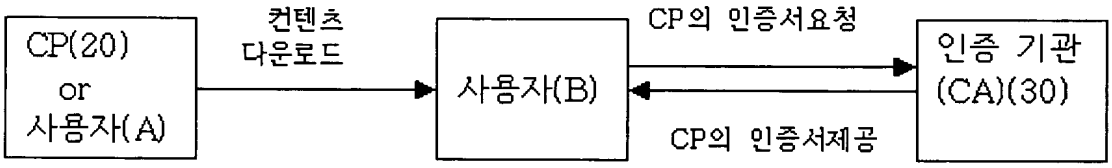
【도 1】


헤더부(Header)(3)
- 컨텐츠 제공자 이름
- 컨텐츠 아이디(ID)
- 라이센스 제공자 URL
- 컨텐츠 메타 정보
- 기타
1
전자서명(Signature)(4)
암호화된 컨텐츠부(2)

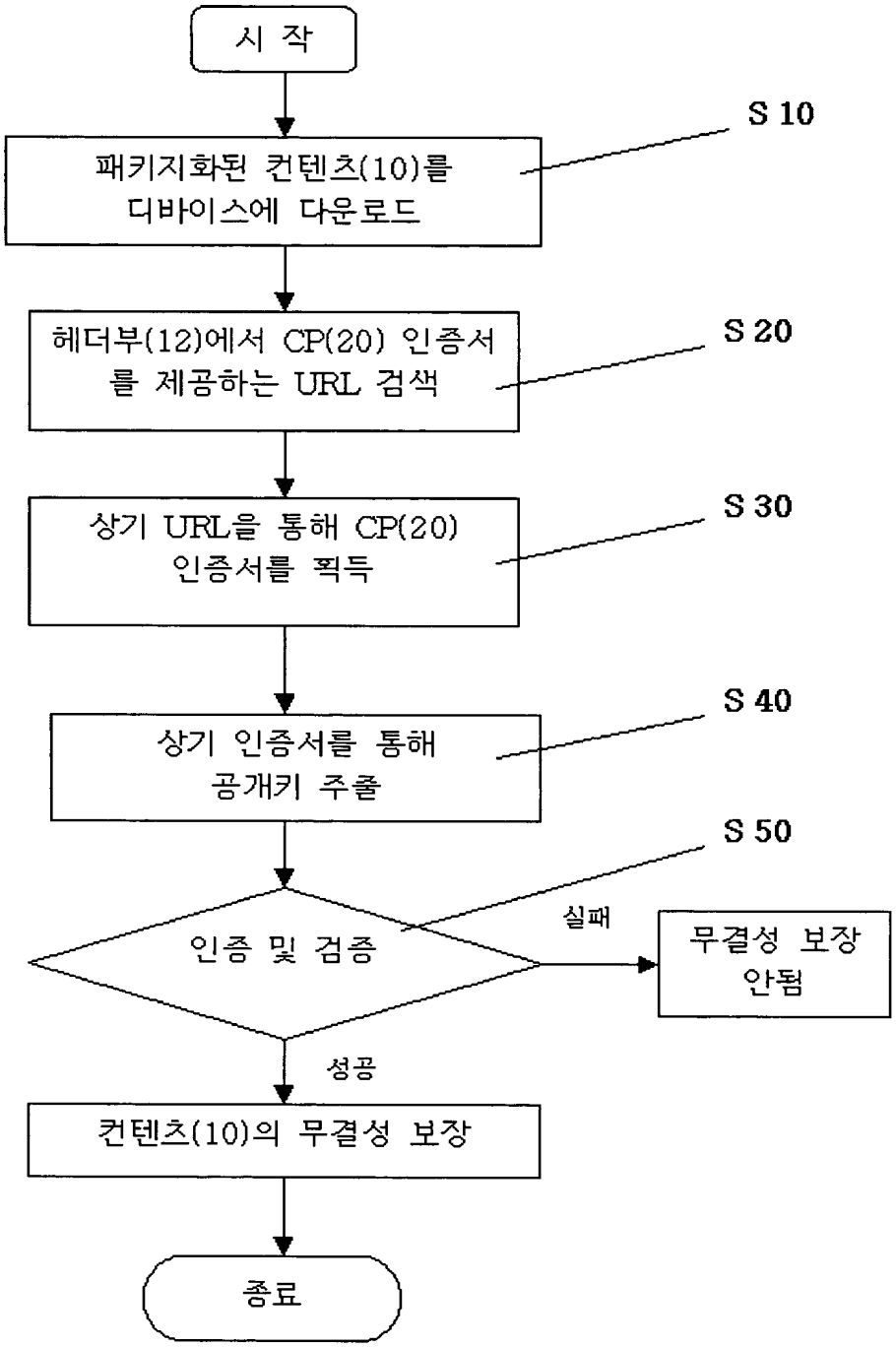
【도 2】


헤더부(Header)(12)
- 컨텐츠 제공자 이름
- 컨텐츠 아이디(ID)
- 라이센스 제공자 URL
- 컨텐츠 메타 정보
- 컨텐츠 제공자 인증서 URL
- 기타
10
전자서명(Signature)(13)
해쉬:헤더부(12)/컨텐츠부(11)
암호화된 컨텐츠부(11)

【도 3】


CP(20)
or
사용자(A)
컨텐츠
다운로드
사용자(B)
CP의 인증서요청
CP의 인증서제공
인증 기관
(CA)(30)

【도 4】


시 작
S 10
패키지화된 컨텐츠(10)를 디바이스에 다운로드
S 20
헤더부(12)에서 CP(20) 인증서를 제공하는 URL 검색
S 30
상기 URL을 통해 CP(20) 인증서를 획득
S 40
상기 인증서를 통해 공개키 추출
S 50
인증 및 검증
실패
무결성 보장 안됨
성공
컨텐츠(10)의 무결성 보장
종료